Amendments To Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for registering biometric information for use in a smartcard system having a biometric security device, said method comprising:

communicating with a smartcard, wherein said smart card comprises a common application and a second application, said second application storing travel-related information associated with a cardholder, said second application comprising a common file structure and a partner file structure;

receiving a first proffered biometric sample and a second proffered biometric sample at a sample receiver, wherein said first proffered biometric sample is a different type of biometric sample from said second proffered biometric sample, and wherein said first proffered biometric sample and said second proffered biometric sample are from the same user, and wherein said first proffered biometric sample is required to access said common file structure and said second proffered biometric sample is required to access said partner file structure;

verifying said first proffered biometric sample and a second proffered biometric sample;

generating data representing said first proffered biometric sample and said second proffered biometric sample;

receiving user information and smartcard information at said sample receiver; and

associating said first proffered biometric sample and said second proffered biometric sample with said user information and said smartcard information to create a data packet; and

enabling write access to a field within said partner file structure upon verification of said second proffered biometric sample and upon request by a first partnering organization;

denying write access to said field upon request by a second partnering organization;

enabling write access for said first partnering organization and said second partnering organization to a field in said common file structure, upon verification of said first proffered biometric sample;

transferring common data to facilitate said registration; and,

transferring said travel-related information, information related to said common file structure and information related to said partner file structure to facilitate said registration.

~~using said data representing said proffered biometric sample as a variable in an encryption calculation to secure at least one of said user information, said smartcard information and transaction data.~~

2. (Currently Amended) The method of claim 1, wherein said step of receiving said first proffered biometric sample and said second proffered biometric sample at said sample receiver includes said sample receiver contacting at least one of a computer, Internet, software, hardware, a third-party biometric entity, a kiosk, a biometric registration terminal, and a communication device.

3. (Currently Amended) The method of claim 1, ~~wherein said step of receiving said proffered biometric sample further includes at least one of: processing, storing, comparing, and verifying said proffered biometric sample~~ further comprising using data representing said first proffered biometric sample and said second proffered biometric sample as a variable in an encryption calculation to secure data related to said registration.

4. (Currently Amended) The method of claim 1, wherein said step of associating said first proffered biometric sample and said second proffered biometric sample with said user information and said smartcard information further includes associating said first proffered biometric sample and said second proffered biometric sample with at least one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

5. (Currently Amended) The method of claim 1, further comprising using said data representing said first proffered biometric sample and said second proffered biometric sample as at least one of a private key, a public key, and a message authentication code to facilitate ~~transaction~~ registration security measures.

6. (Currently Amended) The method of claim 1, further comprising using said data representing said first proffered biometric sample and said second proffered biometric sample in generating a message authentication code and as at least one of a private key and a public key.

7. (Currently Amended) The method of claim 1, wherein said step of associating said first proffered biometric sample and said second proffered biometric sample with said user information and said smartcard information includes associating ~~different~~ said first proffered biometric sample and said second proffered biometric sample with a different one of: personal information, charge

card information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

8. (Currently Amended) The method of claim 1, wherein said step of associating said first proffered biometric sample and said second proffered biometric sample with said user information and said smartcard information includes primarily associating said first proffered biometric sample with a first user information, wherein said first user information comprises at least one of personal information, credit card information, charge card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and secondarily associating said second proffered biometric sample with a second user information, wherein said second user information comprises at least one of personal information, credit card information, charge card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, wherein said second user information is different than said first user information.

9. (Currently Amended) The method of claim 1, wherein said step of associating said first proffered biometric sample and said second proffered biometric sample with said user information and said smartcard information includes associating ~~a~~ said first proffered biometric sample with a first user information, wherein said first user information comprises at least one of personal information, credit card information, charge card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and facilitating registration of ~~a~~ said second proffered biometric sample by associating said second proffered biometric sample with a second user information, wherein said second user information comprises at least one of personal information, credit card information, charge card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

10. (Currently Amended) The method of claim 1, wherein said step of associating said first proffered biometric sample and said second proffered biometric sample with said user information and said smartcard information includes associating ~~a~~ said first proffered biometric sample with a first user information, wherein said first user information comprises at least one of personal information, credit card information, charge card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and associating ~~a~~ said second proffered biometric sample with a second user information, wherein said second user information comprises at least one of personal information, charge card information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, wherein said second user information is different than said first user information.

11. (Currently Amended) The method of claim 1, wherein said step of associating said first proffered biometric sample and said second proffered biometric sample with said user information and said smartcard information includes associating a plurality of proffered biometric samples with user information, wherein each proffered biometric sample is associated with different user information.

12. (Currently Amended) The method of claim 1, further comprising verifying said first proffered biometric sample and said second proffered biometric sample using a secondary identification by facilitating the use of a secondary security procedure.

13. (Currently Amended) The method of claim 1, further comprising using said data representing said first proffered biometric sample and said second proffered biometric sample to facilitate substantially simultaneous access to goods and initiation of authentication for a subsequent purchase of said goods.

14. (Currently Amended) The method of claim 1, wherein said step of receiving said first proffered biometric sample and said second proffered biometric sample at said sample receiver includes receiving said first proffered biometric sample and said second proffered biometric sample at least one of: a local database, a remote database, a portable storage device, a host system, an issuer system, a merchant system, a fob issuer system, an employer, a financial institution, a non-

financial institution, a loyalty point provider, a company, the military, the government, a school, a travel entity, a transportation authority, a POS and a security company.

15. (Currently Amended) The method of claim 1, wherein said step of receiving said first proffered biometric sample and said second proffered biometric sample includes receiving at least one of: a retinal scan, an iris scan, a fingerprint scan, a hand print scan, a hand geometry scan, a voice print scan, a vascular scan, a facial scan, an ear scan, a signature scan, a keystroke scan, an olfactory scan, an auditory emissions scan, and a DNA scan.

16. (Currently Amended) The method of claim 1, wherein said step of associating said first proffered biometric sample and said second proffered biometric sample with said user information and said smartcard information includes associating a preset transaction limit with said first proffered biometric sample and said second proffered biometric sample and at least one of a charge card account, credit card account, debit card account, savings account, private label account and loyalty point account.

17. (Cancelled)

18. (Currently Amended) The method of claim 1, ~~associating said data packet with at least one of a partner file structure and a common file structure stored on a smartcard having an integrated circuit device comprising a common application and a second application, said second application being configured to store travel related information associated with a cardholder;~~

~~said second application comprising said common file structure and said partner file structure, wherein said partner file structure provides write access to a field within said partner file structure for a first partnering organization and denies write access to said field for a second partnering organization, and said common file structure provides write access for said first partnering organization and said second partnering organization to a file in said common file structure;~~ wherein said user information comprises user preferences relating to at least one of rental cars, hotel reservations, and air travel and said data packet is stored in said first partner file structure.

19. (Currently Amended) The method of claim 1, wherein said first proffered biometric sample and said second proffered biometric sample is associated with at least two accounts, wherein each of said at least two accounts includes at least one of: a charge card account, a credit card account, a debit card account, a savings account, a private label account and a loyalty point account.

20. (Currently Amended) The method of claim 18 , further comprising writing to at least one of said partner file structure and said common file structure to program said smartcard as a room key, upon verification of said first proffered biometric sample and said second proffered biometric sample.

21. (Previously Presented) The method of claim 16, wherein said preset transaction limit comprises at least one of a maximum transaction amount, minimum transaction amount, maximum number of transactions within a time period, maximum number of transactions, use by certain merchants, temporal limitation, geographic limitation, and use of non-monetary funds.

22. (New) The method of claim 1, further comprising:

storing, by a first enterprise data collection unit, update registrations and pending registrations associated with said smartcard and a first enterprise, wherein said first enterprise data collection unit is associated with a first enterprise;

storing, by a second enterprise data collection unit, update registrations and pending registrations associated with said smartcard and a second enterprise, wherein said second enterprise data collection unit is associated with a second enterprise;

interfacing with said smartcard and said first and second enterprise data collection units, at an access point;

storing, by a card object database system coupled to said first and second enterprise data collection units, said smartcard information in accordance with said update registrations and said pending registrations, wherein said smartcard information includes a card object having an application;

routing, by an update logic system, said smartcard information from said first and second enterprise data collection units to said access point in order to effect synchronization of said smartcard information associated with said smartcard and said card object database system; and,

activating, by said verification device, said update logic system upon verification of said first proffered biometric sample and said second biometric sample.

23. (New) The method of claim 22, further comprising securely routing, by an update logic system, card information between said enterprise data synchronization interface and said enterprise data collection units, wherein said update logic system is coupled to an enterprise data synchronization interface, and communicating, by said enterprise network, with said access point, wherein said enterprise data synchronization interface is coupled to said enterprise network.

24. (New) The method of claim 23, further comprising, by a secure support client server, communicating with said access point, and adaptively providing communication functionality in accordance with the communication functionality available at said access point.

25. (New) The method of claim 24, further comprising:

communicating, by a key system, with a security server and supplying a key in response to a request from said security server, wherein said key system is associated with said application;

receiving, by a personalization utility, said card object and communicating with said security server;

adding, by said personalization utility, said key to said card object;

accepting, by a card management system, a card request and communicating said card request to said personalization utility; and

communicating, by a gather application module, with said card management system and gathering application information from a first database and a second database in accordance with said card request, wherein said first database is associated with said first enterprise, and said second database is associated with said second enterprise.

26. (New) The method of claim 1, further comprising displaying a first plurality of financial accounts upon verification of said first proffered biometric sample, and displaying a second plurality of financial accounts upon verification of said second biometric sample, wherein said first plurality of financial accounts include different financial accounts than said second plurality of financial accounts.

27. (New) The method of claim 1, further comprising associating a first set of rules with said first proffered biometric sample and displaying a first plurality of financial accounts upon verification of said first proffered biometric sample and said first set of rules, and associating a second set of rules with said second proffered biometric sample and displaying a second plurality of financial accounts upon verification of said second biometric sample and said second set of rules, wherein said first plurality of financial accounts include different financial accounts than said second plurality of financial accounts.